

UNITED STATES PATENT APPLICATION

**METHOD AND APPARATUS FOR ENHANCED SECURITY
IN A BROADBAND TELEPHONY NETWORK**

INVENTORS:

William A. Aiello

Steven Michael Bellovin

Charles Robert Kalmanek, Jr.

William Todd Marshall

Aviel D. Rubin

09516236 030100

Cross Reference to Related Applications

This application claims priority to United States Provisional Application Serial No. 60/122,481, filed on March 1, 1999, and United States Provisional Application Serial No. 60/129,476, filed on April 15, 1999, the contents of which are incorporated by reference herein.

This application is related to Provisional Patent Application entitled "Telephony on a Broadband Network," Serial No. 60/071,346, filed on January 14, 1998; Provisional Patent Application entitled "Telephony Over Broadband Access Networks," Serial No. 60/073,251, filed January 30, 1998; Provisional Patent Application entitled "Distributed Open Signaling Architecture," Serial No. 60/095,288, filed August 4, 1998; and Provisional Patent Application entitled "Distributed Open Signaling Architecture," Serial No. 60/104,878, filed October 20, 1998, the contents of which are incorporated herein by reference.

09:46:36.030400

METHOD AND APPARATUS FOR ENHANCED SECURITY IN A BROADBAND TELEPHONY NETWORK

Field of the Invention

5 The present invention relates generally to communication networks, and more particularly to enhanced security in a broadband telephony network.

Background of the Invention

10 Broadband communication networks provide a viable alternative to present local exchange carrier (LEC) loops in providing both voice and data transmission services. A variety of broadband network architectures have emerged as supporting Internet and telephony access: including cable distribution networks, ISDN (Integrated Services Digital Network), broadband ISDN, DSL
15 ("Digital Subscriber Line"), ADSL, etc.

 A major concern for such broadband communication networks is the need for adequate security measures. The system architecture must ensure user privacy across the network medium and prevent unauthorized access to services. For example, in the case of cable modems based on the Data Over Cable
20 Service Interface Specification ("DOCSIS", a term referring to the ITU-T J.112 Annex B standard for cable modem systems), security is provided by the DOCSIS Baseline Privacy Interface ("BPI") which addresses some of the vulnerability presented by the shared cable network. BPI provides security mechanisms, including encryption using the Cipher Block Chaining (CBC) mode of the Data
25 Encryption System (DES) and key exchange based on RSA encryption, that defend against an eavesdropping threat in the cable network. The successor to BPI, DOCSIS 1.1 Baseline Privacy Interface Plus ("BPI+") adds authentication based on digital certificates that binds media access control addresses for cable modems to RSA public keys. DOCSIS cable modems must be pre-certified with
30 cryptographic keys and/or certificates installed in the hardware at manufacturing time. DOCSIS cable modems undergo a registration process and a baseline

35

40

50

Summary of the Invention

60

It is another object of the present invention to protect the privacy and integrity of signaling and media traffic. It should not be possible to inject
65 signaling traffic into the network that appears to be from another source. It should also not be possible for unauthorized people to eavesdrop on traffic of other users. This includes traffic analysis by which, for example, an attacker can determine who is talking to whom.

It is another object of the present invention to protect the integrity
70 of the called number. It should not be possible to force a called number to another number. This is necessary to prevent a range of attacks on the service, including one in which an attacker tries to steal business from a competitor by causing calls to be misrouted.

It is another object of the present invention to abide by government
75 wiretap laws, e.g. the Communications Assistance for Law Enforcement Act of 1994 ("CALEA"). This may include supplying signaling information and media streams to the authorities. If encryption keys are mediated by the service provider, they must also be supplied to the authorities.

It is another object of the present invention to discourage denial of
80 service attacks. It should not be easier than it is in the existing PSTN for one user or set of users to prevent other legitimate users from obtaining service.

It is another object of the present invention to provide the correct
functionality of conventional telephony features. Subscriber features must function correctly. For example, caller ID information must be included in all
85 calls due to trace requirements. Only users that subscribe to the service should have access to the information. Users should not be able to forge such information in the case of a trace.

It is another object of the present invention to provide an administrative level. There should advantageously be at least two levels of
90 privilege to the system. This is so that decisions such as invoking emergency procedures or downloading new code to customer equipment cannot be performed by all users. For example, in an emergency, administrators must have the ability to preempt a call, while non-administrators should not have this ability.

Thus, in accordance with the present invention, an architecture for
95 using a broadband telephony interface ("BTI") is provided with enhanced security
features. The BTI registers itself with the network in a secure fashion, so that it
can be authenticated and known to the network from then on. A security
association is created by having the BTI generate a cryptographic key (symmetric
or otherwise) and send it to the network under the public key of the network
100 service provider. The two ends can then use this key to establish a secure
connection, and the BTI can send authorization information such as a credit card
number over the secure connection. The cryptographic key can then be used to
derive subsidiary keys that are used for subsequent communications. By having
the BTI generate its own cryptographic key, instead of having a certificate
105 installed at manufacturing time, this allows for the possibility of a BTI
implemented as software. The BTI advantageously need not be a trusted or
certified box; indeed, a software package executed on a personal computer can
fulfill the same functions. This is in contrast to the cable modem, for example,
which must be certified to ensure correct behavior and fair access to the medium.

110 These and other advantages of the invention will be apparent to
those of ordinary skill in the art by reference to the following detailed description
and the accompanying drawings.

Brief Description of the Drawings

115 Fig. 1 is a diagram of a broadband communication network which
can be utilized with an embodiment of the present invention.

Fig. 2 is a block diagram of the components of a hardware
broadband telephony interface configured for use with a preferred embodiment of
the present invention.

120 Fig. 3 is an abstract diagram of a communication provisioning
protocol in accordance with a preferred embodiment of the present invention.

Detailed Description

With reference to Fig. 1, a diagram of a broadband communication network is shown which can be utilized with an embodiment of the present invention. A packet-switched IP backbone 100 is shown connected to access networks 150 and 151, here shown as cable distribution networks, and to a more conventional telephony network 135, here shown as the public switched telephone network ("PSTN"). A broadband telephony interface ("BTI") 170 is shown which provide a gateway between one or more telephones 190 and the packet-switched network. The BTI 170 may be physically integrated with a cable modem ("CM") 160, as shown in Fig. 1, to provide the necessary functions to interface between one or more phone lines and the depicted cable access network 150. The cable modem 160 can also be used by other communication devices 180 (in Fig. 1 shown for example as a personal computer) to connect to the access networks 150. The access network 150 terminates on a cable modem termination system ("CMTS") 155 at a head end. The CMTS 155 interfaces to an Internet Protocol ("IP") edge router ("ER") 120 that connects to a managed IP backbone 100, which provides the connectivity to other BTIs (e.g. 171 with corresponding edge router 121, CMTS 156, access network 151, cable modem 161, communication device 181, and telephone 191) and to gateways 130 to the PSTN 135. A "gate controller" 110 provides authentication, authorization, and call routing functions for calls originated by BTIs. The authentication information used by the gate controller is made available to it by a provisioning process that is described in further detail below. The backbone provides connectivity to a provisioning server 140, which is involved in provisioning the BTI and other network elements.

The particular architecture set forth in Fig. 1 is for illustration purposes only and is further described in the following commonly assigned patent applications: Provisional Patent Application entitled "Telephony on a Broadband Network," Serial No. 60/071,346, filed on January 14, 1998; Provisional Patent Application entitled "Telephony Over Broadband Access Networks," Serial No. 60/073,251, filed January 30, 1998; Provisional Patent Application entitled "Distributed Open Signaling Architecture," Serial No. 60/095,288, filed August 4,

1998; and Provisional Patent Application entitled "Distributed Open Signaling
155 Architecture," Serial No. 60/104,878, filed October 20, 1998, the entire contents
of which are incorporated herein by reference.

Note that although a limited number of network entities are shown
in Fig. 1 for simplicity of presentation, other network entities can obviously be
included in the network – such as additional interface units, routers, controllers,
160 and gateways. Although Fig. 1 sets forth a particular broadband telephony
architecture, one of ordinary skill in the art would recognize that the security
enhancements of the present invention are readily extendible to other
architectures. For example, the present invention can be utilized with broadband
communication networks that do not use cable access networks but rather use
165 digital subscriber line (DSL), Integrated Services Digital Network (ISDN), or
some other access architecture. Moreover, the present invention can be utilized
with other packet-switched architectures or with a hybrid network architecture.

Fig. 2 sets forth a simplified block diagram of the components of a
BTI, configured for use with the present invention. The BTI performs signaling
170 and call control functions and enables telephony service on the communication
network by digitizing, compressing, and packetizing analog signals from a
telephone 190 into data packets for transport over the communication network.
The functions of a BTI can be implemented in many different ways that would be
apparent to one of ordinary skill in the art, including as software executed on a
175 typical computer. Fig. 2 illustrates a hardware embodiment of a BTI 170 that can
be a stand-alone device, can be integrated with a telephone 190 to create a stand-
alone telephony device or can be integrated with an access device (e.g. the cable
modem 160 in Fig. 1 or a set top box) to form a general network interface unit.
The BTI in Fig. 2 comprises a processor 210 and hardware (here shown as a
180 subscriber line interface circuit 250, codec 260, and echo canceler 265) capable of
detecting changes in state information (e.g. hook state detection), collecting dialed
digits (e.g. dual tone multifrequency (DTMF) signals), and participating in the
implementation of telephone features. The processor 210 has access to memory
220 which stores data such as cryptographic keys 222 and the operating system

185 221 and program instructions necessary for the operation of the BTI. For security
purposes, it is advantageous for the BTI also to have read only memory 230 which
stores code downloading code ("CDC") 232 and the service provider's public key
231, as further discussed below. It is also advantageous for some of the data and
code in memory 220 to be stored in some form of non-volatile memory so that
190 such information is not erased if power to the BTI is turned off.

The BTI 170 advantageously should be able to performing
probabilistic computation, whether by hardware (e.g. a noisy diode), software
(e.g. a pseudo-random generator with a good seed), or some combination. This is
necessary for the BTI to be able to generate cryptographic keys and to perform
195 related cryptographic functions such as ElGamal signatures. Without a hardware
source of randomness, it will likely be necessary for the BTI 170 to maintain
about 200 bytes of state for the lifetime of the device, which will need to change
often. One possible embodiment would be to keep the state data in RAM memory
which gets copied to nonvolatile flash memory when there is a chance of a loss of
200 power.

As further elaborated on below, the BTI 170 need not necessarily
be under the direct control of the service provider, e.g. the entity operating the
communication network. The BTI, operated in accordance with the present
invention, can be implemented as customer premises equipment that is untrusted
205 and operates based on locally-stored software. The customer, in other words, can
purchase the BTI at a local store or can have the device shipped to her home.
Where the BTI is implemented as software, it can be simply downloaded and
installed on a computer pre-configured for access to the communication network.

210 Provisioning

In accordance with a preferred embodiment of the present
invention, Fig. 3 illustrates security protocols to be utilized in the provisioning of
a user who wishes to utilize the network. The following notation and
abbreviations are used in the discussion:

215

NOTATION	DEFINITION
SP	A service provider, such as AT&T.
PS	A provisioning server operated by the service provider and reachable over the access network and the backbone.
BTI	The customer premises equipment, namely the broadband telephony interface. The cable modem is not distinguished from the BTI for purposes of the following discussion.
GC	The gate controller. Every BTI communicates with an assigned gate controller on the back end.
U	Refers to the human user.
$\{X\}_{s_{k-}}$	This notation means that the message X is signed with the private portion of public key, k . It is assumed that the public portion, $k+$, is used to verify the signature.
$\{X\}_k$	This indicates that X is encrypted under the key, k .
K_{p-}	This represents the private key of principal, P . So, for example, K_{SP-} is the private key of the service provider.
K_{p+}	This represents the public key of principal, P .
$CERT(ID, k)_{s_{K_{p-}}}$	This represents a public key certificate binding ID to the key k by the authority holding the private key, K_{p-} . We use this notation because certificates can hold a lot of other information.
$A \rightarrow B : message$	This notation means that A sends <i>message</i> to B .
IKE	Internet Key Exchange. This is the Standard protocol for key management defined by the IETF.

In the case of a cable access network 150, it is assumed that the cable modem 160 has undergone DOCSIS registration and the baseline privacy key exchange prior to the provisioning process described below. The cable

220 modem 160 thus has a secure channel with the CMTS 155 at the head end. It is assumed that the network infrastructure beyond the head end is a managed

backbone for which reasonable security precautions have been taken, e.g. to secure servers. The provisioning server 140 itself, since it manages keys, must be very well secured. Nevertheless, it is assumed that the BTI 170 cannot trust
225 signals on the cable. That is, the threat model includes the possibility that a hostile intruder can masquerade as the cable head-end and fool the BTI into believing it is communicating with a legitimate service provider.

In accordance with an embodiment of the present invention, cryptographic means are advantageously utilized to authenticate the service
230 provider. The objective of the provisioning process is for the service provider to securely establish an association between a customer account and a cryptographic key, where the key is available only to the BTI (and the provisioning server). The key can be used to authenticate key exchanges later. In practice, where the key is a symmetric key, this means that the two sides share a string of random bits that
235 can be used as encryption and keys for message authentication codes (MAC). It is common to use different keys to encrypt and MAC in each direction, so if a 128-bit cipher is used, the provisioning scenario will result in at least 512 bits of shared random bits. Note that the cryptographic key can be a public key rather than a symmetric key, where the corresponding private key is stored in the BTI.

240 The service provider, *SP*, is assumed to have a public/private key pair. The private key is stored in a safe place and there are strict procedures for accessing this key. The public key, K_{SP+} , is stored in the memory of the BTI or built into the BTI, for example by burning the key into read only memory. If this public key turns out to be source of attack (e.g. attackers successfully substitute a
245 rogue key into BTIs in a particular area and manage to spook the provisioning server), then the key can be further protected by storing it in tamper-resistant storage. It is advantageous that there be a public key infrastructure whereby the service provider issues public key certificates for the provisioning servers, e.g. *PS*. There can be several layers of hierarchy in practice. It is assumed that the private
250 key for the provisioning server is stored somewhere inside the network, and that when the BTI sends a message to the provisioning server, it is communicating with a secure location inside the network.

The user obtains and installs the BTI, whether by merely plugging the device in or by installing software on a computer. The user picks up the phone and dials a provisioning number (e.g. 611) to enable registration. In accordance with a preferred embodiment of the present invention, the following messages, as illustrated in Fig. 3, then take place. It should be noted that, in addition to or in lieu of the signatures indicated in Fig. 3, the values of the messages can be digitally signed or hashed, using a message authentication code (MAC) with each message. Different keys can be utilized in each direction with the protocol. Such details are not included for simplicity of exposition and would be known to one of ordinary skill in the art.

At step 301, the BTI 170 receives the provisioning number:

U \rightarrow BTI : 611

The BTI issues a SETUP message to the gate controller 110, which routes the call to a provisioning server 140 and returns a SETUP_ACK message containing the IP address of the provisioning server. The authentication information in the SETUP message from the BTI can be null.

At step 302, the BTI 170 announces its existence to the provisioning server 140

BTI \rightarrow PS : yo!

and requests the certificate and public key from the provisioning server 140. At step 303, the provisioning server 140 provides its public key and certificate:

PS \rightarrow BTI : $K_{PS+}, CERT(P, K_{PS+})_{S_{KSP-}}$

Certificates are convenient here because they allow the BTI to store a public key, here the service provider's public key, and have confidence in another public key

(here, the provisioning server's public key) if it carries a certificate signed by the private key corresponding to the service provider's public key stored in the BTI.

285 At step 304, the BTI 170 generates random symmetric keys, SK , AK , and K and transmits the following message to the provisioning server 170:

$$BTI \rightarrow PS : \{SK, AK, N_0\}_K, \{info\}_{SK}, \{K\}_{K_{PS}}$$

290 K is used to encrypt the message that is sent with a symmetric cipher. K itself is encrypted with the public key of PS to make sure nobody else can read it. SK is a session key that will be used for future communication with the provisioning server 170 for the remainder of the provisioning. AK is a symmetric key that is used to secure the audio channel. In practice, AK may actually be a master key
 295 used to generate the actual keys used for encryption and to generate message authentication codes (MAC). N_0 is a random nonce (a one-time identifier) used to prevent replay attacks (it is possible to avoid using nonces by including a hash of the received (challenged) message in every response). The reply from PS will contain N_0 as well to link the two messages together. $info$ contains the
 300 information in the message, such as the network address (Media Access Control address, IP address, etc.) of the broadband telephony interface 170.

At step 305, the provisioning server 140 acknowledges the registration request and proves knowledge of the session key:

305 $PS \rightarrow BTI : \{ACK, N_0, N_1\}_{SK}$

At this point, the session key is "good" and the network associates it with the particular IP endpoint.

At step 306, the BTI 170 sets up a voice connection with the provisioning server 140 and uses the audio channel key, AK , to secure the voice
 310 path. In practice, the audio stream should be encrypted and protected using message authentication codes. For simplicity, the secure messages, M , on the

audio channel are represented as $\{M\}_{AK}$. At this point, the BTI 170 completes the setup of the voice connection to the provisioning server 140.

315 At step 307, the provisioning server 140 prompts the user for her authentication information:

PS \rightarrow U : {"enter auth info"}_{AK}

320 The authentication information can be implemented in many different ways. For example, the authentication information can be a work order number that has been given to a customer (or to an installer) after the customer has subscribed for the service. The work order must be supplied when the BTI is provisioned to identify the customer account. As another example, the authentication information can be
325 a credit card number, address, etc. that is provided by the user who subscribes for the service during the provisioning call itself. The audio stream is secured using AK from the PS 140 to the BTI 170, which converts it to an analog voice for the user.

 At step 308, the user speaks or dials her authentication information
330 in response to the prompt:

U \rightarrow BTI : *auth info*

 At step 309, the BTI 140 sends the authentication information over the secure
335 audio channel to the provisioning server 140:

BTI \rightarrow PS : {auth info}_{AK}

 At step 310, the BTI 140 generates a public/private key pair for the
340 user and sends the public key, K_{U+} , to the provisioning server 140.

BTI \rightarrow PS : $\{N_1, N_2, K_{U+}\}_{SK}$

345 The provisioning server 140 associates the authentication information sent over the secure audio channel with the public key, K_{U+} , sent over the secure control channel. The PS 140 can do this because (a) it is aware that both came from the same network address and (b) it successfully authenticates and decrypts both the audio and control channel information using the keys, AK and SK, which the PS knows are associated with the same broadband telephony interface 170. The PS
350 140 stores the BTI's public key for later usage and acknowledges receipt:

$$PS \rightarrow BTI : \{ACK, N_2\}_{SK}$$

355 At this point, the user is provisioned. The BTI 170 and the provisioning server 140 share a long-term symmetric key that the provisioning server can associate with the subscriber account. In practice, the BTI and PS may share up to 512 random bits to comprise four 128-bit encryption and MACing keys, as described above. In future sessions, the BTI 170 can generate a session key, sign it, and send it under the public key of the provisioning server 140 or the long-term key it
360 shares with the server in a similar manner. No interaction from the user is necessary to establish these future session keys.

The foregoing Detailed Description is to be understood as being in every respect illustrative and exemplary, but not restrictive, and the scope of the
365 invention disclosed herein is not to be determined from the Detailed Description, but rather from the claims as interpreted according to the full breadth permitted by the patent laws. It is to be understood that the embodiments shown and described herein are only illustrative of the principles of the present invention and that various modifications may be implemented by those skilled in the art without
370 departing from the scope and spirit of the invention.